

THE CHOI LAW GROUP, LLC
100 Challenger Road, Ste 302
Ridgefield Park, New Jersey 07660
Telephone: (201) 438-0200
Telefax: (201) 623-5888
Attorneys for *Plaintiff*

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

-----X

JKSOFT, INC., a California corporation,

Civil Action No.:

Plaintiff,

COMPLAINT

v.

INNOAS, INC., a New Jersey corporation,
SEUNG JAI YI, a/k/a NOAH LEE, and John
Does 1-20, being fictitious names presently
unknown to the Plaintiff and ABC Corporations
21-40, being fictitious names presently
unknown to the Plaintiff,

Defendants.

-----X

Plaintiff JKSOFT, INC., a California corporation, by way of Complaint against
Defendants INNOAS, INC., a New Jersey corporation, NOAH LEE, and John Does 1-10, being
fictitious names presently unknown to the Plaintiff and XYZ Corps. 11-30, being
fictitious names presently unknown to the Plaintiff, (collectively referred to herein as the
“Defendants”), hereby alleges as follows:

INTRODUCTION

1. This is an action for copyright infringement; contributory copyright infringement;
common law trademark infringement; violation of the Computer Fraud and Abuse Act (CFAA);
violation of the Digital Millennium Copyright Act (“DMCA”); violation of the Federal Defense

of Trade Secret Act (“DTSA”); unfair competition; permanent injunction; and, various other state law claims.

2. These claims arise from Defendants’ unlawful sale and distribution of Plaintiff’s Point of Sale software and Product Licensing/Activation Keys (hereafter “Key” or “Keys”) for various software created and sold by the Plaintiff, including JKRestaurant, JKRetail and JKSalon (collectively referred to as the “POS software”). The Keys in question have been pirated by Defendants. Upon information and belief, Defendants obtained the source code to the POS software through either hacking or unauthorized copying of the POS software source code and/or Plaintiff’s Key creation program or the decryption of the "license.key" file which is located in the Key’s document folder, by Noah Lee and/or someone who aided and abetted his wrongful conduct. The POS software and Key creation program were created and developed by Jae H. Kang, who is the owner and Principal of the Plaintiff. The activation Key creation software is password protected. In order to use it, Noah Lee, or someone acting on his behalf, would need to hack the password to run it.

3. Defendants thereafter unlawfully sold and distributed Plaintiff’s POS Sale software together with the counterfeit and pirated Keys to allow customers access to the full version of the software.

4. A Key, or Product Key, is a specific software/hardware-based key for a computer program. It is akin to a serial number and certifies that the copy of the program is original and is legally licensed. Keys consist of a unique series of numbers and/or letters. Plaintiff is the only person that is authorized to manufacture the Keys. Keys must be entered into the end-user’s computer that runs the POS Software in order to gain access to the full version of the software. Keys are typically used by software developers to protect their intellectual property from piracy

and other forms of abuse. Keys in and of themselves do not constitute a software license, however, they are needed to activate the software for end-users to use legally purchased and licensed software. The Keys do not constitute authorization from a software developer to access or use software unless the software is specifically and legally purchased and licensed.

5. Plaintiff does not issue Keys without the accompanying legally purchased and licensed POS software.

6. At no relevant time herein has Plaintiff authorized, permitted or consented to Defendants selling or distributing the counterfeit or pirated Keys to be used to activate Plaintiff's POS software.

7. Upon information and belief, Defendants knew, intended, and impermissibly instructed their sub-dealers and customers to use the counterfeit and pirated Keys to activate unlicensed copies of Plaintiff's POS software.

8. Upon information and belief, Noah Lee personally participated in and had the ability to supervise, direct, and control the wrongful conduct alleged in this Complaint, and he and his company, Innoas, derived a direct financial benefit from that wrongful conduct. Both Noah Lee and Innoas are therefore liable for the wrongful conduct alleged herein.

THE PARTIES

9. Plaintiff JKSoft, Inc. (hereinafter "JKSoft" and/or "Plaintiff") is California corporation, with its headquarters located at 3429 W Olympic Blvd. #502, Los Angeles, California. Jae H. Kang ("Kang"), also known as Brian Kang (i.e., Kang's American name), is the owner and Principal of JKSoft. In fact, the "JK" in JKSoft, JKRestaurant, JKRetail and JKSalon are derived from Kang's initials.

10. Upon information and belief, Defendant Innoas, Inc. (“Innoas”), is a New Jersey corporation, with its principal place of business located at 21 Grand Avenue, Suite 111, Palisades Park, New Jersey 07650.

11. Upon information and belief, Defendant Seung Jai Yi, a/k/a Noah Lee (“Lee”) is the Principal of Defendant Innoas, and is presently residing at 527 Green Valley Road, Paramus, New Jersey 07652

12. John Does 1-20, being fictitious names of individuals whose identity and/or whose participation and/or culpability is presently unknown to the Plaintiff, and intended to represent those individuals who intentionally violated Plaintiff’s intellectual property rights and/or aided, abetted and assisted Defendants in illegally procuring, selling, and distributing Plaintiff’s POS software together with pirated Keys.

13. John Does 21-40, being fictitious names of corporate entities whose identity and/or whose participation and/or culpability is presently unknown to the Plaintiff, and intended to represent those corporate entities who intentionally violated Plaintiff’s intellectual property rights and/or aided, abetted and assisted Defendants in illegally procuring, selling and distributing Plaintiff’s POS software together with counterfeit and pirated Keys.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction under 17 U.S.C. § 501, 28 U.S.C. §§1331 and 1338(a) and the Computer Fraud Act; and, the Court also has subject matter jurisdiction under 28 U.S.C. § 1332 because this action is between citizens of different states and the matter in controversy exceeds \$75,000, exclusive of interest and costs

15. Venue is proper in this Court pursuant 28 U.S.C. §1391 and 28 U.S.C. § 1400(a) since the Defendants are residents of and/or conducts substantial business, and may be otherwise

found, within this Judicial District. Additionally, substantially all of the acts giving rise to Plaintiff's causes of action occurred within this Judicial District.

16. This Court has personal jurisdiction over the Defendants because the Defendants reside and/or conduct substantial business activities and engage in the commission of tortious acts within this Judicial District.

FACTS COMMON TO ALL CLAIMS

17. Kang met Noah Lee ("Lee") in or around 2005 when Lee has just moved to the United States, upon information and belief. Kang was then living in New Jersey. Kang, and his then partner, owned and operated a different software company from the Plaintiff herein at that time.

18. Kang hired Lee as a sales representative because Lee was quite personable and demonstrated a skill for sales. However, Lee's employment with that company did not last long. Lee accompanied Kang to a trade show at which Kang was there as an Exhibitor. Kang brought a computer with him so he could perform quick updates to the software. To be clear, the software referred to in this paragraph is not the software that is the subject of this litigation. Nevertheless, after the tradeshow, Lee became intoxicated and confessed to Kang that he had copied Kang's software's "source code" to a USB memory stick at one point when Kang had stepped away.

19. The software's source code is the most important form of intellectual property to a software company. Lee told Kang that he had copied it out of curiosity. At the time, Kang believed Lee's excuse, but after informing his partner about what had happened, Kang's partner terminated Lee's employment.

20. In or around 2007, Kang ran into Lee and they renewed their relationship. In fact, they then began what Kang thought of as a very close friendship. Lee told Kang that he had

hired a computer programmer to develop a salon point of sale software, but he was not satisfied with what the programmer had developed. Thus, Kang agreed to develop a point of sale software from scratch without referencing to the work of the programmer that Lee hired, which he would sell to Lee who, in-turn, would be permitted to sell to third-parties (e.g., end-users).

21. Kang completed the JKSalon point of sale software in 2007, and he began selling copies to Lee's company. At the time, Lee was doing business through a company known as Zionlink. Lee subsequently created a new business – i.e., Innoas – whereafter Kang began selling the POS software to Innoas. Kang subsequently created JKRestaurant and JKRetail. Kang also sold the POS software to other authorized dealers who are commonly referred to as Value Added Resellers or "VARs."

22. When the program is installed and opened, an end-user would see their name displayed on the software screen, as well as the name JKSoft. JKSalon, JKRestaurant or JKRetail would also be displayed on screen depending on which POS software they were using.

23. After Kang finished developing the POS software, and because there were other VARs who would be selling the POS software, Lee asked Kang if he would make a modification to the POS software that Plaintiff sold to Zionlink. Specifically, Lee asked if "ZionPOS", "ZionBeauty" and later "Innoas" name appear and be displayed on the screen instead of JKSoft's name. Lee said he needed this exclusive modification in order to give him some perceived distinct advantage over the other VARs.

24. Kang agreed to the modification request by Lee. Kang also agreed to sell the POS software to Lee at a discounted price. Because the Key was needed to activate the full version of the software, which meant Lee (or his company) would still have to pay for the software and sign the licensing agreement, Kang was not too concerned about Lee's request. Furthermore, all

Kang needed to accommodate Lee's request was to add a temporary file to the installation directory, which could also be easily deleted to reveal the underlying JKRestaurant, JKRetail or JKSalong software products. In fact, "right-clicking" on the JKRestaurant.exe, JKSalon.exe or JKRetail.exe, click file in "Properties," and then selecting the "Version" tab, reveals that the file was created by JKSoft and the name of the product appears as JKRestaurant, JKRetail or JKSalon.

25. In essence, this file modification equated to placing Innoas' name tag over the JKSoft name. All versions sold to other VARS did not have this modification. Kang, however, subsequently learned that Lee was using this modification to mislead potential customers and sub-dealers by claiming that his company developed the software.

26. Defendants purchased the earlier version of the POS software, which is more prone to error since the software has not been matured yet. Thus, Plaintiff continued to sell it to Defendants at the \$250.00 discounted price, instead of the \$500.00 regular price per copy. Like other dealers, Innoas requested POS software updates throughout the years, although much less frequently than other dealers. Innoas then stopped requesting these updates in 2017, which was when Plaintiff began noticing the significant increase in the Keys being pirated and counterfeited. This leads Plaintiff to suspect that Innoas has been using a counterfeit copy of the software too.

27. Kang moved to Los Angeles in late 2007. In 2008, Kang incorporated JKSoft in California and created the JKRestaurant and JKRetail software, which was likewise sold to end-users via VARS, including Defendants.

28. As set forth above, Kang and Lee developed what Kang thought of as a very close friendship. Lee attended Kang's wedding. Lee also stayed at Kang's home when visiting Los Angeles and *vice versa*. In fact, Lee visited Kang in Los Angeles several times from 2008

through 2016. Significantly, Kang's home also serves as JKSoft's business office. Thus, JKSoft's software development computer is located there.

29. In 2013, Kang initiated a tracking process of the Keys and noticed that there were counterfeit and pirated Keys reporting back the registration data containing the unrecognizable serial number (hereafter "data") to his computer. Based upon his review, Kang determined that the counterfeit and pirated Keys started to be first used in or around 2011-2012 – although he was not able exactly ascertain in which years each was specifically sold since he only started the tracking in 2013. Commencing in 2013, Plaintiff noticed that some of the information being returned by its software had Key registrations with serial # not found in its database. After 2013, the number of pirated Keys began to decline and JKSoft decided not to pursue an investigation into the individual(s) responsible for the pirated Keys, who were then unknown to JKSoft.

30. During the period of 2014-2016, only a handful of new counterfeit and pirated Keys were reporting data back to the Plaintiff. Thus, Plaintiff decided to gather more evidence before investigating it. Notwithstanding the foregoing, Kang suspected that it was Lee and Innoas responsible for the counterfeit and pirated Keys because this behavior was only occurring in the geographic region in which Innoas was the primary dealer.

31. However, and as a result of Kang's foregoing suspicions and Innoa's unfair pricing practices to its sub-dealers, in March 2017, Plaintiff advised Innoas that it would no longer sell the POS software and Keys to Innoas at a discounted rate, and Innoas would have to pay the same price as the other VARS. Contrary to Kang's reasonable expectations that Innoas would either dispute the pricing increase with Kang or try to resolve the pricing issues directly with its-sub dealers, Innoas instead completely stopped purchasing the POS software and

requesting Keys from the Plaintiff and began to create, distribute and sell the counterfeit or pirated license Keys.

32. Thereafter, in 2017, approximately 204 new counterfeit and pirated Keys began reporting back data to Plaintiff's computer from Innoas' geographic region, including a few from Rhode Island, Connecticut and Massachusetts. Plaintiff was told by a third-party that Innoas was still selling the Keys to its sub-dealers as of the end of the year 2017 although it was January 2017 when Innoas last purchased the Keys from JKSoft.

33. All in total, 274 counterfeit and pirated keys have reported registration data to Plaintiff's computer since Plaintiff began tracking this data in 2013. Again, Innoas was the primary authorized dealer in the region where this behavior occurred. Innoas was also using sub-dealers to assist in this geographic region.

34. In December 2017, Plaintiff learned from a third-party that in or about 2013, Lee told this individual that he had Plaintiff's source code. Lee also admitted to this individual that he created counterfeit and pirated Keys.

35. As set forth in Paragraph 2 above, Kang suspects that Lee either illegally gained access to Kang's computer files through an open wifi network in Kang's home (i.e., Lee somehow "hacked" in); or Lee used a USB memory stick, like he did once before, to copy, the JKSoft software's source code and/or the Key creation program. Likewise, the "license.key" file could have been possibly decrypted and reverse engineered.

JKSoft's Intellectual Property

36. Plaintiff develops, maintains, advertises, markets, distributes, and licenses several point of sale computer software programs, such as JKRestaurant, JKReatil and JKSalon, which have since been copyrighted as set forth above. JKRestaurant, JKReatil and JKSalon software,

which are not just the brand names, graphics, display screens, titles and marks belonging to JKSoft, although the same has not yet been registered for trademark.

37. One prevalent form of software piracy involves the unauthorized and unlawful distribution of fake or pirated activation Keys. The use of these fake Keys generates substantial illicit revenues for unlawful sellers of them. Furthermore, many purchasers of these Keys are legitimate businesses who are deceived and unaware that they are not acquiring genuine and licensed software.

38. Thus, similar to other software developers, Plaintiff has implemented initiatives to protect its customers and combat theft of its intellectual property. One such initiative is its' Key which enables the activation of the POS software. Because the POS software is capable of being installed on multiple computers, Plaintiff relies on the product Key process to detect piracy and protect consumers from the risks of non-genuine software.

39. Plaintiff uses VARS to sell and distribute its POS software. The full version of the POS software cannot be fully activated until it is paid for by the VARS and a legitimate Key is plugged to the end-users computer. The Key is basically a unique serial # on a USB stick which Plaintiff sells to the VARS. The VARS then plugs the Key to the end-users computer. Significantly, no title or rights to ownership of the software passes to the VARS or end-user.

40. Plaintiff's Key contains an encrypted multi-character alphanumeric string created by the Plaintiff via a Key creation program that Plaintiff also developed. Accordingly, Keys are a necessary component of the software because, without them, the software cannot be totally unlocked and is useable only in a "demo" mode in which certain features or functions of the software are limited or restricted.

41. When Plaintiff creates a Key, it records various information onto its database, including but not limited to the following:

Product Name

Date license key was created

USB memory stick's unique hardware serial #

USB memory stick's drive serial #

Name of computer that generated the license key; and,

Name of Dealer who purchased the license key; etc..

42. Additionally, after the Key is installed on an end-user's computer, Plaintiff's POS software sends registration information – i.e., data - back to Plaintiff's database in order to protect its intellectual property rights, which includes, but is not limited to, the following information:

The name of the business using the software

The product name

Date license key was created

USB memory stick's unique hardware serial #

USB memory stick's drive serial #

Name of computer that generated the license key; and,

Name of the dealer who purchased the license key, etc.

43. By directing the software to report back this information, the Plaintiff is able to determine whether the product is legally licensed and/or is a pirated. JKSoft can then cross-reference this information with the licenses legally issued because each customer's key is unique.

44. As set forth above, Plaintiff is aware that the Keys were counterfeited and pirated because the data being reported back to Plaintiff's computer could not be cross-referenced to the unique serial # from JKSoft's Key manufacturing database because they were missing some critical information such as the name of the dealer who purchased the license key, name of the computer that created the Key and more importantly, the creation dates were fake.

45. JKSoft did not authorize Defendants to sell or distribute its software with pirated or counterfeit Keys.

46. Commencing in or around 2011-2012, and with an exponential increase in frequency in 2017, the Defendants deliberately avoided purchasing Keys from the Plaintiff, choosing instead to create, distribute and sell fake, counterfeit and pirated copies of the Plaintiff's Key in violation of Plaintiff's intellectual property rights.

47. In doing so, Defendants then distributed the counterfeit and pirated Keys directly to individual consumers or sub-dealers.

48. At the time that Defendants distributed and sold the counterfeit and pirated Keys, Defendants knew, or should have known, that they were infringing upon Plaintiff's intellectual property rights.

49. Defendants also knowingly directed, supervised, and controlled the infringement of Plaintiff's intellectual property rights by their sub-dealers.

50. Defendants had a direct financial interest in, and stood to gain a direct financial benefit from, their deliberately infringing activity.

51. By engaging in the illegal conduct alleged above, in addition to directly organizing and effectuating such infringing activities, Defendants also personally induced,

caused, and materially contributed to infringing conduct by others, including end-users to whom Defendants sold the pirated Keys.

52. While Plaintiff believes it has located most of the end-users who are using the counterfeit and pirated Keys, Defendants' infringing activities are ongoing and appear to be rampant. Plaintiff believes that there might be substantially more counterfeit and pirated Keys being used. For example, if some end-users do not have internet access or, Innoas somehow blocked the software's outbound internet access, monthly Key registrations cannot report data to JKSoft. Further, Plaintiff also noticed some counterfeit and pirated Key registration data without store names being identified. This indicates that Defendants deliberately did not enter store names in POS software in order to hide the location of counterfeit and pirated Key and who is using it.

53. Defendants' wrongful conduct also includes the use of Plaintiff's marks, name, and/or imitation visual designs (specifically displays, logos, icons, graphic designs, and/or packaging). These items constitute the intellectual property belonging to the Plaintiff. They have each been used on a continuous basis in interstate commerce to identify and distinguish Plaintiff's POS software as of the date of first use in commerce by the Plaintiff.

54. In December 2017, Plaintiff forwarded a "Cease and Desist" Letter to end-users of the counterfeit and pirated keys. Defendants' brazen reply, reflects that Defendants will continue to infringe upon the Plaintiff's intellectual property rights.

55. More specifically, Defendants are claiming, that Innoas has a contractual right to continue to sell the POS software, with the counterfeit and pirated Key. Defendants also appear to be claiming that it possesses an ownership interest in the POS software as either the owner thereof or co-developer. This representation is untrue. Again, as set forth above, the POS

software is essentially accessible through various distributors, but only in demo mode. The Key is what unlocks the entire programs, and that Key must be legally purchased with the POS software.

FIRST COUNT

Copyright Infringement Under 17 U.S.C. §§ 101, 501 et seq.

56. Plaintiff re-alleges and incorporates by reference the allegations set forth above in paragraphs 1 through 55.

57. Plaintiff's software and its Key constitute original works that are copyrightable subject matter pursuant to the Copyright Act, and they are protected by registrations duly issued to Plaintiffs (or their predecessors or affiliates) by the United States Copyright Office.

58. At all relevant times, Plaintiff has been and still is the owner, or exclusive licensor, of all rights, title, and interest in and to its copyrights in its intellectual property, which has never been assigned or otherwise transferred to Defendants.

59. Beginning on an unknown date in 2013 and continuing to the present, Defendants, with knowledge of Plaintiff's ownership interest in its intellectual property, began infringing upon Plaintiff's copyrights. Specifically, Defendants created fake Keys to unlock the full version of Plaintiff's POS software. They did so by, among other things, selling the pirated Keys directly to customers and/or sub-dealers who, in-turn, sold them to customers without Plaintiff's permission, license, or consent.

60. Defendants are infringing upon the Plaintiff's copyrights by selling, distributing, using and offering for sale pirated copies of Plaintiff's key in this Judicial District without approval or authorization from Plaintiff.

61. Defendants' conduct is willful, deliberate, knowing, intentional and malicious and, at a minimum, Defendants acted with willful blindness to and in reckless disregard of Plaintiff's copyrights.

62. As a result of Defendants' unlawful and deliberate conduct as set forth above, Plaintiffs have been, and will continue to be, damaged.

63. Plaintiff is entitled to recover damages, which include any and all profits Defendants have made as a result of their wrongful conduct under 17 U.S.C. § 504. Alternatively, Plaintiff is entitled to statutory damages under 17 U. S.C. § 504(c).

64. In addition, for the reasons set forth above, the award of statutory damages should be enhanced in accordance with 17 U.S.C. § 504(c)(2).

65. Plaintiff is also entitled to injunctive relief pursuant to 17 U.S.C. § 502 and to an order impounding any and all infringing materials pursuant to 17 U.S.C. § 503. Plaintiff has no adequate remedy at law for Defendants' wrongful conduct. Plaintiff's copyrights are unique and valuable property which has no readily determinable market value. Defendants' infringement harms Plaintiff and its products such that Plaintiff cannot be made whole by any monetary award. Furthermore, Defendants' wrongful conduct, and the resulting damage to Plaintiff and its licensees is continuing.

66. Plaintiff is also entitled to recover its attorneys' fees and costs of suit under 17 U.S.C. § 505.

SECOND COUNT

Contributory Copyright Infringement Under 17 U.S.C. §§ 501, et seq.

67. Plaintiff re-alleges and incorporates by reference the allegations set forth above in paragraphs 1 through 66.

68. Defendants have contributed to the infringement of Plaintiff's copyrights by distributing pirated Keys in the United States of America without approval, authorization, consent or license from Plaintiff to sub-dealers and end users and directing those sub-dealers and end users to activate Plaintiff's software that they were not licensed to use without the legally purchased Keys.

69. At a minimum, Defendants acted with willful blindness to, or in reckless disregard of, Plaintiff's copyrights.

70. Upon information and belief, Defendants have committed, and continue to commit, acts contributing to the copyright infringement of Plaintiff's intellectual property.

71. Plaintiff is entitled to recover damages, which include any and all profits Defendants have made as a result of their wrongful conduct under 17 U.S.C. § 504. Alternatively, Plaintiff is entitled to statutory damages under 17 U. S.C. § 504(c).

72. In addition, for the reasons set forth above, the award of statutory damages should be enhanced in accordance with 17 U.S.C. § 504(c)(2).

73. Plaintiff is also entitled to injunctive relief pursuant to 17 U.S.C. § 502 and to an order impounding any and all infringing materials pursuant to 17 U.S.C. § 503. Plaintiff has no adequate remedy at law for Defendants' wrongful conduct. Plaintiff's copyrights are unique and valuable property which has no readily determinable market value. Defendants' infringement harms Plaintiff and its products such that Plaintiff cannot be made whole by any monetary award. Furthermore, Defendants' wrongful conduct, and the resulting damage to Plaintiff and its licensees is continuing.

74. Plaintiff is also entitled to recover its attorneys' fees and costs of suit under 17 U.S.C. § 505.

THIRD COUNT

Common Law Trademark Infringement

75. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 74 above as if set forth at greater length herein.

76. This action for common law trademark infringement against the Defendants is based on Defendants' use of Plaintiff's marks, logos, product names, etc. in commerce in connection with the distribution, sale, and/or offering for sale of goods, materials and/or services bearing some or all of the Plaintiff's marks in violation of Plaintiff's common law trademark rights.

77. The Defendants are continuously, directly and contributorily, infringing upon the Plaintiff's marks, etc., with deliberate intent or willful blindness, and they continue to mislead the public into assuming a connection between the counterfeit products, materials and services and Plaintiff's marks.

78. The Defendants' counterfeiting and infringing activities are likely to cause and actually are causing confusion, mistake, and deception among members of the trade and the general consuming public as to the origin and quality of the goods, materials and services sold and/or rendered under the Plaintiff's marks.

79. The Defendants' unlawful actions have caused and are continuing to cause irreparable injury and damages to Plaintiff and its licensees, and the Defendant has been unjustly enriched.

FOURTH COUNT

State Trademark Dilution (N.J.S.A. § 56:3-3.20)

80. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 79 above as if set forth at greater length herein.

81. Defendants acts set out above are likely to dilute the distinctive quality of the Plaintiff's marks and Defendants are in violation of N.J.S.A. § 56:3-13.20.

82. Defendants acts set out above have caused, and unless enjoined by this Court, will continue to cause great and irreparable injury to Plaintiff.

83. Plaintiff has no adequate remedy at law.

FIFTH COUNT

Violation of the Computer Fraud and Abuse Act Under 18 U.S.C. § 1030

84. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 83 above as if set forth at greater length herein.

85. Plaintiff engages in internet commerce because it does not maintain a typical "brick and mortar" retail outlet. Its business operations, including, but not limited to, advertising, communications, are conducted primarily through the internet. Plaintiff uses its computers in interstate and/or foreign commerce or communication.

86. Plaintiff's computers and those of Kang, who often works from home developing Plaintiff's software, is where Plaintiff maintains and stores its proprietary, confidential information and trade secrets. On these computers, plaintiff maintains the source codes for its various POS Software and its Key creation software.

87. Plaintiff's computers are protected within the broad definition and meaning of The Computer Fraud and Abuse Act, commonly referred to as the "CFAA", 18 U.S.C. § 1030, which was enacted by Congress to combat increasingly common computer-related crimes.

88. The CFAA prohibits any person from, *inter alia*, : (a) "access[ing] a protected computer without authorization" so as to perpetuate a fraud and "obtain anything of value"; (b) knowingly "caus[ing] the transmission of a program, information, code or command" so as to intentionally cause damage to a protected computer; (c) accessing a protected computer without authorization, in a manner that causes "damage" to the computer; or (d) causing damage to a protected computer through the unauthorized transmission of computer passwords.

89. In or about 2013, Defendant Lee illegally accessed Plaintiff's computer(s) by hacking Kang's wifi network or by using a USB memory stick to download the source code to Plaintiff's POS software and/or Plaintiff's Key creation programs. Defendants, or someone with programming skills assisting and acting in concert with Defendants, could then copy the Plaintiff's source code and/or license key creation program once they decrypted the password protecting it. Also, they could have decrypted the "license.key" file in the license key itself.

90. By accessing Plaintiff's computers, without authorization, or in excess of the authorization permitted by Kang, the computers of the Plaintiff and/or Kang, Defendants knowingly and with the intent to defraud obtained valuable information from protected computers as defined by the CFAA in violation of 18 U.S.C. §§ 1030 (a)(2)(c) and 1030 (a)(5)(c).

91. As a result of this unauthorized access to Plaintiff's and/or Kang's computers, Defendants downloaded, transferred and stole, with the intent to defraud, Plaintiff's valuable

information (i.e., its intellectual property), including confidential and proprietary information as well as trade secrets.

92. The CFAA, 18 USC §1030(g), also expressly recognizes a civil cause of action for compensatory damages or injunctive relief by a person who “suffers damage or loss by reason of a violation of the Act.

93. As a result of Defendants’ conduct, Plaintiff has suffered damages and/or loss in excess of \$5,000 in the one (1) year period immediately preceding the date of this filing, and the damages continue to grow.

94. Plaintiff is also entitled to injunctive relief or other equitable relief under the CFAA.

SIXTH COUNT

Violation of the Digital Millennium Copyright Act (“DMCA”) under 17 U.S.C. § 1201

95. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 94 above as if set forth at greater length herein.

96. Plaintiff owns copyrights in its intellectual property, which has never been assigned or otherwise transferred to Defendants.

97. Plaintiff at all relevant times has employed technological measures to block unauthorized access to the full version of Plaintiff’s POS software including the Keys and identification system to monitor any unauthorized access thereto or access through counterfeit Keys, etc.

98. On information and belief, Defendants are infringing upon the Plaintiff’s copyrights by selling, distributing, using and offering for sale pirated copies of Plaintiff’s key that has been designed or produced for the purpose of circumventing technological measures

and/or protection afforded by the technological measures that has been employed by Plaintiff to control access to the full version of its POS software.

99. Defendants' counterfeit or pirated Keys have no or limited commercially significant purpose or use other than to circumvent the technological measures that effectively control access to the full version of Plaintiff POS software.

100. Defendants' unlawful and deliberate conduct set forth above has caused irreparable and incalculable harm to Plaintiff and will continue to cause irreparable and incalculable harm for which Plaintiff has no adequate remedy at law.

101. Plaintiff is entitled to the relief provided by 17 U.S.C. § 1201-1203, including, but not limited to, injunctive relief, compensatory and/or statutory damages, punitive damages, and Plaintiff's costs and attorneys' fees.

SEVENTH COUNT

Violation of the Federal Defense of Trade Secret Act ("DTSA") under 18. U.S.C. § 1836

102. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 101 above as if set forth at greater length herein.

103. Plaintiff's POS software has been used or is intended to be used in various states in the United States including but not limited to, New York, New Jersey, Rhode Island, Connecticut and Massachusetts, and therefore, the product embodying the Plaintiff's intellectual property has been used in interstate commerce or is intended to be used in interstate commerce.

104. On information and belief, the intellectual property embodying the Plaintiff's POS software are the trade secrets which is entitled to protection under the DTSA because: 1) Plaintiff's intellectual property includes technical, business, program devices, methods, procedures, programs or codes for which the Plaintiff as the owner has taken reasonable

measures to keep such information secret by implementing technical features such as a separate software access key requiring the Plaintiff's authorization or approval thereof, and ; 2) such technical information have not been generally known to, and not being readily ascertainable through proper means by another person.

105. Defendants' unlawful and deliberate conducts in creating counterfeit or pirated Keys have been or are intended to gain unlawful access to the Plaintiff's trade secrets because Defendants has had or has no proper means to gain access to such information.

106. Defendants' unlawful and deliberate conducts have caused and will continue to cause irreparable harm to Plaintiff.

107. Plaintiff is entitled to the range of relief provided by 18. U.S.C. § 1832 – 1836, including but not limited to, injunctive relief, compensatory and/or statutory damages, punitive damages, and Plaintiff's costs and attorneys' fees.

EIGHT COUNT

Statutory Unfair Competition Under N.J.S.A. § 56:4-1 et Seq.

108. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 107 above as if set forth at greater length herein.

109. Defendants' acts set out above constitutes unlawful, unfair, or fraudulent business practices in violation of N.J.S.A. § 56:4-1 et seq.

110. Defendants are unlawfully promoting and otherwise selling, using, distributing and offering for sale Plaintiff's POS software and counterfeit pirated Keys, which constitute Plaintiff's copyrighted Intellectual Property.

111. Defendants' conduct constitutes unfair competition with Plaintiff's authorized dealers under the laws of New Jersey. This conduct is causing immediate and irreparable injury

to Plaintiff and to its goodwill and reputation, and will continue both to damage Plaintiff and to deceive the public unless enjoined by this Court. Plaintiff has no adequate remedy at law.

112. The natural, probable, and foreseeable consequence of the Defendants' wrongful conduct have been and will continue to be the deprivation of the exclusive rights Plaintiff has in and to its intellectual property.

113. Defendants' acts have injured and will continue to injure Plaintiffs by, among other things, siphoning customers, diluting Plaintiff's Intellectual Property, confusing customers and injuring Plaintiff's reputations.

114. As a result of the above-described wrongful activities of unfair competition by the Defendants, Plaintiff has suffered, and will continue to suffer, irreparable injury to its goodwill and reputation, resulting in substantial damages, and the Defendants have been unjustly enriched.

115. Upon information and belief, Defendants have profited from their unlawful acts.

116. Plaintiff has no adequate remedy at law.

NINTH COUNT

Violation of the Computer Fraud and Abuse Act Under 18 U.S.C. § 1030

117. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 116 above as if set forth at greater length herein.

118. Plaintiff engages in internet commerce because it does not maintain a typical "brick and mortar" retail outlet. Its business operations, including, but not limited to, advertising, communications, are conducted primarily through the internet. Plaintiff uses its computers in interstate and/or foreign commerce or communication.

119. Plaintiff's computers and those of Kang, who often works from home developing Plaintiff's software, is where Plaintiff maintains and stores its proprietary, confidential

information and trade secrets. On these computers, plaintiff maintains the source codes for its various POS Software and its Key creation software.

120. Plaintiff's computers are protected within the broad definition and meaning of The Computer Fraud and Abuse Act, commonly referred to as the "CFAA", 18 U.S.C. § 1030, which was enacted by Congress to combat increasingly common computer-related crimes.

121. The CFAA prohibits any person from, *inter alia*, : (a) "access[ing] a protected computer without authorization" so as to perpetuate a fraud and "obtain anything of value"; (b) knowingly "caus[ing] the transmission of a program, information, code or command" so as to intentionally cause damage to a protected computer; (c) accessing a protected computer without authorization, in a manner that causes "damage" to the computer; or (d) causing damage to a protected computer through the unauthorized transmission of computer passwords.

122. In or about 2013, Defendant Lee illegally accessed Plaintiff's computer(s) by hacking Kang's wifi network or by using a USB memory stick to download the source code to Plaintiff's POS software and/or Plaintiff's Key creation programs. Defendants, or someone with programming skills assisting and acting in concert with Defendants, could then copy the Plaintiff's source code and/or license key creation program once they decrypted the password protecting it. Also, they could have decrypted the "license.key" file in the license key itself.

123. By accessing Plaintiff's computers, without authorization, or in excess of the authorization permitted by Kang, the computers of the Plaintiff and/or Kang, Defendants knowingly and with the intent to defraud obtained valuable information from protected computers as defined by the CFAA in violation of 18 U.S.C. §§ 1030 (a)(2)(c) and 1030 (a)(5)(c).

124. As a result of this unauthorized access to Plaintiff's and/or Kang's computers, Defendants downloaded, transferred and stole, with the intent to defraud, Plaintiff's valuable information (i.e., its intellectual property), including confidential and proprietary information as well as trade secrets.

125. The CFAA, 18 USC §1030(g), also expressly recognizes a civil cause of action for compensatory damages or injunctive relief by a person who "suffers damage or loss by reason of a violation of the Act.

126. As a result of Defendants' conduct, Plaintiff has suffered damages and/or loss in excess of \$5,000 in the one (1) year period immediately preceding the date of this filing, and the damages continue to grow.

127. Plaintiff is also entitled to injunctive relief or other equitable relief under the CFAA.

TENTH COUNT

Common Law Unfair Competition

128 Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 127 above as if set forth at greater length herein.

129. Defendants are unlawfully selling, offering for sale, using and distributing Plaintiff's POS software, together with a counterfeit and pirated Key, without Plaintiff's authorization or consent.

130. Defendants have injured Plaintiff by depriving it of sales of the POS software and by injuring their business reputation and by passing off the POS software, and counterfeit and pirated Keys, as their own. Defendants' conduct is likely to confuse a prospective customer

exercising ordinary caution or to cause mistake or to deceive the public into believing that the POS software and counterfeit and pirated Keys are the intellectual property of the Defendants.

131. Defendants are unlawfully promoting and otherwise selling, using, distributing and offering for sale Plaintiff's POS software and counterfeit and pirated Keys, which constitute Plaintiff's copyrighted Intellectual Property.

132. Defendants' conduct constitutes unfair competition with Plaintiff's authorized dealers under the common law of New Jersey. This conduct is causing immediate and irreparable injury to Plaintiff and to its goodwill and reputation, and will continue both to damage Plaintiff and to deceive the public unless enjoined by this Court. Plaintiff has no adequate remedy at law.

133. The natural, probable, and foreseeable consequence of the Defendants' wrongful conduct have been and will continue to be the deprivation of the exclusive rights Plaintiff has in and to its intellectual property.

134. Defendants' acts have injured and will continue to injure Plaintiffs by, among other things, siphoning customers, diluting Plaintiff's Intellectual Property, confusing customers and injuring Plaintiff's reputations.

135. As a result of the above-described wrongful activities of unfair competition by the Defendants, Plaintiff has suffered, and will continue to suffer, irreparable injury to its goodwill and reputation, and substantial damages, and the Defendants have been unjustly enriched.

136. Upon information and belief, Defendants have profited from their unlawful acts.

137. Plaintiff has no adequate remedy at law.

ELEVENTH COUNT

Tortious Interference With Economic Interest

138. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 137 above as if set forth at greater length herein.

139. By virtue of Defendants sale and distribution of Plaintiff's POS software with counterfeit and pirated Keys, Defendants have avoided paying the Plaintiff for the right to legally sell and distribute the same thereby interfering with the present and future economic interests of Plaintiff.

140. Plaintiff has a reasonable expectation of economic advantage and the growth of its business relative to the development, sales and distribution of its POS software.

141. Defendants intentionally, maliciously, and without justification or excuse unreasonably and actually interfered with Plaintiff's pursuit of its legitimate business objectives free from undue influence or molestation.

142. Based upon the foregoing, Defendants interfered with the present and future economic interests of the Plaintiff.

143. As a direct and proximate result of the conduct of Defendants, Plaintiffs have and will continue to be caused to suffer economic damages.

TWELFTH COUNT

Conversion

144. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 143 above as if set forth at greater length herein.

145. Defendants have wrongfully sold and distributed Plaintiff's POS software and Key to third-parties.

146. Upon information and belief, Defendants have received monetary compensation for the sale and distribution of the same.

147. In light of the foregoing, Defendants have wrongfully, inappropriately and illegally converted property in which Plaintiff possessed ownership interest.

148. As a direct and approximate result thereof, Plaintiff has suffered damages and loss in an amount to be determined by the Court.

149. Defendants are liable to the Plaintiff for said damages.

THIRTEENTH COUNT

Civil Conspiracy To Defraud

150. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 148 above as if set forth at greater length herein.

151. Upon information and belief, Defendants conspired, schemed and agreed by, between and/or among themselves to defraud, took steps to defraud and did defraud the Plaintiff of its interest in POS software, its' Key and economic benefits arising therefrom.

152. As a direct and proximate result of the acts of civil conspiracy, Plaintiff has been caused to suffer damages.

153. Defendants are liable to Plaintiffs for Defendants' conspiratorial acts in an amount to be determined by the Court.

FOURTEENTH COUNT

Unjust Enrichment

154. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 152 above as if set forth at greater length herein.

155. Defendants are infringing upon Plaintiff's intellectual property rights

156. Upon information and belief, Defendants are benefitting financially from their wrongful conduct.

157. Defendants are selling copies of Plaintiff's POS software and Key without remitting payment to the Plaintiff.

158. Defendants are also effectively competing with Plaintiff in the sale and distribution of Plaintiff's POS software and, upon information and belief, is underselling Plaintiff's VARS because he is not paying for the same because he is using a counterfeit and pirated Key to unlock the program.

159. The reasonable value of wrongful conduct of Plaintiff is presently incapable of being calculated until an accounting is performed.

160. As a result of the foregoing, Defendant has been unjustly enriched by virtue of her wrongful conduct.

FIFTEENTH COUNT

Accounting

161. Plaintiff hereby repeats and re-alleges the allegations set forth in Paragraphs 1 through 160 above as if set forth at greater length herein.

162. Pursuant to common law as well as 17 U.S.C. § 504, Plaintiff is entitled to an accounting to ascertain and recover any and all profits of Defendants that are attributable to their acts of infringement.

163. The amount of money due from Defendants is presently unknown to Plaintiff and cannot be ascertained without an accounting of the Defendants' books and records regarding their sales and distribution of Plaintiff's POS software and Key.

WHEREFORE, Plaintiffs demand judgment as follows:

1. An *ex parte* temporary and preliminary injunction be issued enjoining Defendants, any of its respective officers, agents, privies, shareholders, principals, directors, licensees, attorneys, servants, employees, affiliates, subsidiaries, successors and assigns, and all those persons in concert or participation with any of them, and any entity owned or controlled in whole or substantial part by the Defendant from:

(a) Using, copying, distributing, processing or advertising any of Plaintiff's trademarked or copyrighted POS software, and counterfeit and pirated POS software and/or license/activation Keys (as described in the Complaint), trade names, materials or services, including but not limited to those identified in the Complaint above, or any simulation, reproduction, copy, colorable imitation or confusingly similar variation of any of Plaintiff's trademarks or trade names or copyrighted materials, or as part of any design or logo or otherwise on or in connection with any goods or on or in connection with the importation, promotion, advertisement, sale, offering for sale, manufacture, production, dissemination or distribution of any goods;

(b) Utilizing any of Plaintiff's copyrighted and trademarked or POS software trade names in connection with any advertising and promotions;

(c) Engaging in any other activity constituting an infringement of any of Plaintiffs' trademarks, trade names or copyrighted materials;

(d) Engaging in any activity that dilutes or tarnishes, or is likely to dilute or tarnish, any of Plaintiffs' trademarks or trade names or copyrighted materials;

(e) Applying to register or registering Plaintiff's Trademark or Copyrighted materials in the United States Trademark and/or Copyright Offices.

(f) Assisting, aiding, or abetting any other person or business entity in engaging in or performing any of the activities referred to in subparagraphs (a) through (e) above or taking any action that contributes to any of the activities referred to in subparagraphs (a) through (e) above, or any other activity that consists of or contributes to the sale of counterfeit or infringing products bearing any of Plaintiff's trademarks or trade names or copyrighted materials.

2. Directing Defendants to turn over to the Plaintiff all counterfeit and pirated software and/or Keys (as described in the Complaint) and other copyrighted or trademarked materials used in violation of Plaintiff's exclusive copyrights as well as all related, electronically stored information used to create the pirated and counterfeit POS software and Keys (as described in the Complaint) records and documents and, at final judgment, destruction or other reasonable disposition of the unlawfully used materials, including digital files and any other means by which they could be used again by Defendants without Plaintiff's authorization.

3. That Defendants be ordered to, at their own expense, immediately deliver up for destruction their entire inventory of goods bearing any of Plaintiff's intellectual property.

4. That Defendants be ordered, at their own expense, to recall and retrieve any and all products that bear any copies or counterfeits of any of Plaintiff's intellectual property and materials from any person to whom they distributed or sold same, and that such recall notices and other actions be taken within five (5) days after service of judgment with notice of entry thereof upon them.

5. That Defendants deliver up to Plaintiff's attorney for destruction, within five (5) days after service of judgment with notice of entry thereof upon them, POS software and Keys (as described in the Complaint), all goods, materials, copies, digital files, promotional and marketing materials, advertisements and other materials (a) currently in their possession or under

their control or (b) recalled by the Defendant pursuant to any order of the Court or otherwise, incorporating, featuring or bearing any of Plaintiff's intellectual property including any simulation, reproduction, copy or colorable imitation of the same, and any other means of making the same, and that Plaintiff be permitted to destroy all such goods without compensation to any of the Defendant.

6. That the Defendants preserve all books, records (including all hard drives on computers used for business purposes, including servers, as well as all computer disks and back up disks) and other documents, whether in electronic format or otherwise, concerning all transactions relating to their sale of any goods bearing or including any copies or counterfeits of any of Plaintiff's intellectual property materials, or any other matter that otherwise infringes upon any of Plaintiff's trademarks or trade names or copyrighted materials, and that all such materials be made available to Plaintiff for review, inspection and copying on Plaintiff's request.

7. That Defendants provide Plaintiff with the names, addresses and all other contact information in their possession (e.g., telephone numbers, fax numbers) for all customers who were sold counterfeit and pirated POS software and Keys (as described in the Complaint).

8. The Defendants shall file with the Court and serve upon Plaintiff's counsel within thirty (30) days after service of judgment with notice of entry thereof upon them a report in writing under oath, setting forth in detail the manner and form in which there has been compliance with all of the above.

9. That Defendant account for and pay over to Plaintiff three times the profits realized by said Defendant from their infringement of the Plaintiff's intellectual property, and their unfair competition with Plaintiff.

10. That Plaintiffs be awarded monetary relief, including Defendants' profits; Plaintiffs' actual damages; trebled damages and/or increased profits, and damages as provided under statute or common law for infringement of said intellectual property; trebled profits or damages, and, if Plaintiff elects, statutory damages as the Court considers just, up to the statutory damages under 17 U.S.C. § 504(c); and punitive and/or enhanced damages as provided for under federal and state law including but not limited to N.J.S.A. 56:4-1, arising out of Defendants' acts of willful trademark and copyright infringement, and counterfeiting, unfair competition and dilution.

11. That Plaintiff be awarded interest, including pre-judgment interest, on the foregoing sums.

12. That Plaintiff be awarded their costs in this civil action, including reasonable attorney's fees and expenses, pursuant to 17 U.S.C. § 501, et seq., and any other applicable laws.

13. That any bank accounts of the Defendants be frozen pending payment to Plaintiff as required hereunder and Plaintiff may execute a judgment against any bank accounts of the Defendant to obtain the amounts required to be paid to Plaintiffs hereunder.

14. That Plaintiff be awarded such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury.

LOCAL RULE 11.2 CERTIFICATION

Pursuant to Local Civil Rule 11.2 of District of New Jersey, the undersigned hereby certifies, upon information and belief, that at the time of filing the within pleading, the

undersigned is not aware that the matter in controversy is the subject of another New Jersey Action nor any other actions pending in any other court, nor of any pending arbitration or administrative proceeding, except as disclosed herein.

DESIGNATION OF TRIAL COUNSEL

Louis M. DiLuzio is hereby designated as trial counsel for Plaintiff.

RESPECTFULLY SUBMITTED,

THE CHOI LAW GROUP, LLC
Attorneys for Plaintiff

By: /s/ Louis M. DiLuzio
LOUIS M. DILUZIO, ESQ.

Dated: January 5, 2018